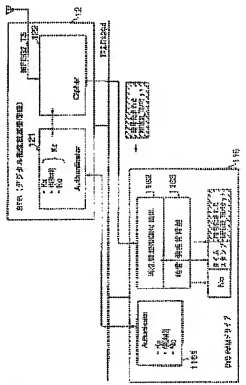
DATA STORAGE DEVICE, RECORDING METHOD OF CIPHERED DATA AND RECORDING MEDIUM

Publication number: JP2000231758 (A)
Publication date: 2000-08-22
Inventor(s): HARUKI KOUSUKE
Applicant(s): TOKYO SHIBAURA ELECTRIC CO
Classification:
- international: ***G11B20/10; G06F12/14; G06F21/24;*** **G11B20/10; G06F12/14; G06F21/00;** (IPC1-7): G11B20/10
- European:
Application number: JP19990032457 19990210
Priority number(s): JP19990032457 19990210

Abstract of **JP 2000231758 (A)**

PROBLEM TO BE SOLVED: To realize a storage system in which a reproducing control for ciphered digital contents is efficiently conducted even though digital contents are ciphered and recorded as they are. SOLUTION: When a digital versatile disk(DVD)-RAM drive 116 receives 1394 packets from a set top box(STB) 12, the drive 116 takes out ciphered MPEG2-TS packets. A reproducing control information adding section 1162 adds a time stamp (time information) for a special reproducing to the ciphered MPEG2-TS packets as reproducing control information. A time varying information control section 1163 adds time varying element information to specify the time variable used to cipher the data to be ciphered in one sector unit, for example. Thus, one sector data recorded in a DVD-RAM medium are constituted of time varying element information (a difference of Nc), a time stamp and a ciphered MPEG2-TS packet group.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－231758
（Ｐ2000－231758Ａ）
(43)公開日　平成12年８月22日(2000.8.22)

(51)Int.Cl.⁷	識別記号	Ｆ１	ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ１１Ｂ　20/10		Ｃ１１Ｂ　20/10	Ｈ　５Ｄ０４４

審査請求　未請求　請求項の数11　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－32457

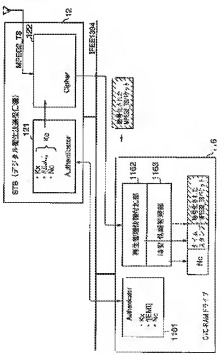
(22)出願日　平成11年２月10日(1999.2.10)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　春木　耕祐
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　５Ｄ０４４ ＡＢ０７ ＢＣ０６ ＣＣ０４ ＤＥ０３ ＤＥ２４
ＤＥ３９ ＤＥ５２ ＥＦ０５ ＧＫ０６ ＧＫ１７
ＨＬ０６ ＨＬ１１

(54)【発明の名称】　データ記憶装置、暗号化データの記録方法および記録媒体

(57)【要約】
【課題】デジタルコンテンツを暗号化したまま記録した場合でも効率よくその再生制御を行うことが可能な記憶形式を実現する。
【解決手段】ＤＶＤ－ＲＡＭドライブ１１６は、ＳＴＢ１２から１３９４パケットを受信すると、そこから暗号化されたＭＰＥＧ２＿ＴＳパケットを取り出す。再生管理情報付加部１１６２は、暗号化されたＭＰＥＧ２＿ＴＳパケットに対して、特殊再生のためのタイムスタンプ（時刻情報）を再生管理情報として付加する。時変情報管理部１１６３は、例えば１セクタ単位で、その暗号化データの暗号化に使用されている時変数を特定するための時変要素情報を付加する。これにより、ＤＶＤ－ＲＡＭメディアに記録される１セクタデータは、時変要素情報（Ｎｃの差分）、タイムスタンプ、および暗号化されたＭＰＥＧ２＿ＴＳパケット群から構成される。



【特許請求の範囲】

【請求項1】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを暗号化したまま記録媒体上に記録するデータ記録装置であって、

前記暗号化されたデータを受信する受信手段と、

この受信手段によって受信された暗号化データを構成する複数の暗号化データユニットのそれぞれに、それら暗号化データユニット間の時間的な順序関係を示す再生管理用情報を付加して前記記録媒体上に記録する記録手段とを具備することを特徴とするデータ記録装置。

【請求項2】　前記暗号化されたデータは、伝送遅延を補償するための所定の時刻情報から構成されるタイムスタンプがそれぞれに付加された複数のパケットに分割されて前記相手先デバイスから送信され、

前記記録手段は、前記受信手段によって受信されたパケットに付加されているタイムスタンプを、前記再生管理用情報として付加して記録することを特徴とする請求項1記載のデータ記録装置。

【請求項3】　前記コピープロテクト対象のデータの暗号化は、時変数と暗号化鍵生成要素として含む暗号化鍵を用いて行われ、

前記記録手段は、前記各暗号化データユニットに、その暗号化に用いられた時変数の値を特定するための時変要素情報を付加する時変要素情報付加手段をさらに含み、

前記暗号化データユニットは前記再生管理用情報および前記時変要素情報が付加された状態で前記記録媒体上に記録されることを特徴とする請求項1記載のデータ記録装置。

【請求項4】　前記暗号化鍵は、前記時変数とそれ以外の他の暗号化鍵要素とを用いて生成されたものであり、

前記記録手段は、前記相手装置との間の認証処理によって取得した前記他の暗号化鍵要素を、通常のデータアクセスでは読み出すことが出来ない前記記録媒体上の所定領域に記録することを特徴とする請求項1記載のデータ記録装置。

【請求項5】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを暗号化したまま記録媒体上に記録するデータ記録装置であって、

前記コピープロテクト対象のデータの暗号化は、時変数を1暗号化鍵生成要素として使用することによって生成された暗号化鍵によって暗号化されており、

前記暗号化されたデータを受信する受信手段と、

この受信手段によって受信された暗号化データを構成する各暗号化データユニットに、その暗号化に用いられた時変数の値を特定するための時変要素情報を付加して前記記録媒体上に記録する記録手段とを具備することを特徴とするデータ記録装置。

【請求項6】　前記記録手段は、同一の時変数を用いて暗号化された1以上の暗号化データ単位で前記時変要素情報を付加して記録することを特徴とする請求項5記載のデータ記録装置。

【請求項7】　コピープロテクト対象のデジタルコンテンツの記録に使用可能なデータ記録装置であって、

前記相手先のデバイスとの間で前記コピープロテクト対象のデジタルコンテンツを扱うことができるデバイスであることを互いに認証するための認証手段と、

この認証手段による認証処理後、前記相手先のデバイスから暗号化されて送信される前記コピープロテクト対象のデジタルコンテンツを受信する受信手段と、

この受信手段によって受信されたデジタルコンテンツの暗号化データに、その特殊再生に必要な時間情報を付加して記録媒体上に記録する手段とを具備することを特徴とするデータ記録装置。

【請求項8】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを暗号化したまま記録媒体上に記録するための暗号化データの記録方法であって、

前記暗号化されたデータを受信し、

受信した暗号化データを構成する複数の暗号化データユニットのそれぞれに、それら暗号化データユニット間の時間的な順序関係を示す再生管理用情報を付加して前記記録媒体上に記録することを特徴とする暗号化データの記録方法。

【請求項9】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを暗号化したまま記録媒体上に記録するための暗号化データの記録方法であって、

前記コピープロテクト対象のデータの暗号化は、時変数を1暗号化鍵生成要素として使用することによって生成された暗号化鍵によって暗号化されており、

前記暗号化されたデータを受信し、

受信した暗号化データを構成する各暗号化データユニットに、その暗号化に用いられた時変数の値を特定するための時変要素情報を付加して前記記録媒体上に記録することを特徴とする暗号化データの記録方法。

【請求項10】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを所定のデータフォーマットを用いることによって暗号化したまま記録する記録媒体であって、

前記コピープロテクト対象の暗号化データは、それを構成する所定の暗号化データユニット単位で、それら暗号化データユニット間の時間的な順序関係を示す再生管理用情報が付加された状態で記録されていることを特徴とする記録媒体。

【請求項11】　相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを所定のデータフォーマットを用いることによって暗号化したまま記録する記録媒体であって、

前記コピープロテクト対象のデータの暗号化は、時変数を1暗号化鍵生成要素として使用することによって生成

された暗号化鍵によって暗号化されており、
前記コピープロテクト対象の暗号化データは、それを構成する所定の暗号化データユニット単位で、その暗号化に用いられた時変数の値を特定するための時変要素情報が付加された状態で記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデジタルコンテンツのコピープロテクションシステムで使用されるデータ記憶装置、暗号化データの記録方法および記録媒体に関する。

【０００２】

【従来の技術】近年、コンピュータ技術の発達に伴い、デジタルビデオプレーヤ、セットトップボックス、ＴＶ、デジタルＶＣＲ、パーソナルコンピュータ等のマルチメディア対応の電子機器が種々開発されている。この種の電子機器は、例えばＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）に蓄積された映画、デジタル衛星放送によるＴＶ番組、等のデジタルコンテンツを扱うことができる。これらデジタルコンテンツは一般にＭＰＥＧ２という動画像高能率符号化方式を使って符号化された後、記録媒体や、伝送媒体を通じて各家庭に送られる。

【０００３】近年、このようなデジタルコンテンツの著作権保護等の観点から、その不正コピーを防止するためのコピープロテクト技術の必要性が叫ばれている。そこで、最近では、マルチメディアデータの伝送に好適な次世代のバスインターフェイスであるＩＥＥＥ１３９４シリアルバスに向けた新たなコピープロテクト方式の検討が進められている。

【０００４】

【発明が解決しようとする課題】ＩＥＥＥ１３９４コピープロテクト技術としては、公開鍵暗号化方式や共通鍵暗号化方式などのよく知られた暗号化プロトコルを用いることによりデジタルコンテンツを暗号化し、その暗号化されたデジタルコンテンツを、ＩＥＥＥ１３９４シリアルバスを介してデジタルビデオプレーヤ、セットトップボックス、ＴＶ、デジタルＶＣＲ、パーソナルコンピュータなどの機器間で受け渡しする仕組みが考えられている。この場合、送信側の機器でコンテンツを暗号化して受信側の機器に送信し、受信側の機器がその暗号化データを復号することになる。

【０００５】しかし、例えばデジタル放送番組などのコンテンツをデジタルＶＣＲやＤＶＤ－ＲＡＭで記録する場合などを考えると、受信側のデジタルＶＣＲやＤＶＤ－ＲＡＭで暗号化を解除してしまうと、生のデータがデジタル記録されてしまうことになり、不正コピーが行われる危険が高くなる。このため、暗号化して送信されるデジタルコンテンツは、本出願人による特許出願である特願平１０－１０８１１８号明細書に記載されているように、暗号化したままデジタルＶＣＲやＤＶＤ－ＲＡＭにデジタル記録することが好ましい。また、特願平１０－１０８１１８号明細書では、暗号化されたデジタルコンテンツの暗号化を解除するための鍵については、システムから話し出すことが出来ない領域に記録することによって、その秘匿化を図っている。

【０００６】ところで、一般に、記録メディアに記録されたデジタルコンテンツの各種再生制御は、そのデジタルコンテンツのソースデータ自体に含まれるアドレスや時間などの再生用管理情報を参照することによって行われている。具体的には、ＤＶＤメディアに記録されているＤＶＤビデオタイトルの場合には、そのソースデータに含まれるビデオオブジェクトのアドレスを参照することによって目的とするビデオデータ部のみをＤＶＤメディアから読み出すことにより、早送り再生、早送り逆再生、マルチシーン再生などの特殊再生を実現している。

【０００７】しかし、上述したように、コピープロテクトの目的でデジタルコンテンツのソースデータ全体を暗号化したままデジタル記録した場合には、そのソースデータの内容を参照することはできない。よって、再生には必要なデータ部のみを読み出すという制御を行うことが出来ないので、再生に使用されないデータも含めて、常に、暗号化されたソースデータ全体を記録メディアからシーケンシャルに読み出さなければならず、再生装置側との間で無駄なデータ転送が生じることになる。また、この場合には、再生装置側には大容量の受信バッファを用意することが必要となり、再生装置のコストアップにつながることになる。

【０００８】また、時変要素値を暗号化鍵として使用するコピープロテクションシステムにおいては、同一コンテンツにおいても、その復号に必要な暗号化鍵は時間と共に逐次変化する。したがって、デジタルコンテンツのソースデータを暗号化したままデジタル記録した場合においては、再生対象の暗号化データ部に応じてそれに対応する時変要素値を再生装置に通知しなければならない。

【０００９】しかし、前述したように暗号化鍵情報の秘匿化のために、その暗号化鍵情報と暗号化データとを別個の領域に記録する方式では、再生対象の暗号化データ部とそれに対応する時変要素値とを同時に読み出すことはできない。このため、再生対象の暗号化データ部が切り替わる度に、それに対応する暗号化鍵情報を別の領域から読み出さなければならない。よって、再生装置側で暗号化鍵の変化を確認しながら、後号・再生をリアルタイムに行うことは実質上困難である。

【００１０】本発明は上述の実情に鑑みてなされたものであり、デジタルコンテンツを暗号化したまま記録した場合でも効率よくその再生制御を行うことが可能なデータ記憶装置、暗号化データの記録方法および記録媒体を

提供することを目的とする。

【0011】

【課題を解決するための手段】上述の課題を解決するため、本発明は、相手先のデバイスから暗号化されて送信されるコピープロテクト対象のデータを暗号化したまま記録媒体上に記録するデータ記録装置であって、前記暗号化されたデータを受信する受信手段と、この受信手段によって受信された暗号化データを構成する複数の暗号化データユニットのそれぞれに、それら暗号化データユニット間の時間的な順序関係を示す再生管理用情報を付加して前記記録媒体上に記録する記録手段とを具備することを特徴とする。

【0012】このデータ記録装置においては、各暗号化データユニットに再生管理用情報を付加してデジタル記録しているため、その再生管理用情報を参照することにより、暗号化データの途中から任意の部分を読み出して再生することができる。したがって、早送り再生、早送り逆再生、マルチシーン再生などの特殊再生時においても、暗号化データ全てを読み出すことなく、その特殊再生に必要な暗号化データ部のみを記録媒体から読み出して再生装置側に送信することが可能となる。

【0013】また、前記暗号化されたデータが、例えばパケット送信時刻などの伝送遅延並を補償するための所定の時刻情報から構成されるタイムスタンプが、それぞれに付加された複数のパケットに分割されて前記相手先デバイスから送信されるようなシステムにおいては、前記記録手段は、前記受信手段によって受信されたパケットに付加されているタイムスタンプを、前記再生管理用情報として使用することができる。これにより、専用の再生管理用情報を生成する処理を省略することができる。

【0014】また、前記コピープロテクト対象のデータの暗号化に、時変数を暗号化鍵生成要素として含む暗号化鍵が使用されている場合には、前記記録手段は、前記各暗号化データユニットに、その暗号化に用いられた時変数の値を特定するための時変要素情報を付加する時変要素情報付加手段をさらに含み、前記暗号化データユニットは前記再生管理用情報および前記時変要素情報が付加された状態で前記記録媒体上に記録されることを特徴とする。

【0015】このように、暗号化データユニットとそれに対応する時変要素情報とをパケット化して記録することにより、時変要素値を暗号化鍵として使用するコピープロテクションシステムにおいても、暗号化データユニットとその復号に必要な時変要素情報とを同時に読み出して再生装置側に送信することが可能となる。

【0016】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【0017】図1には、本発明の一実施形態に係るコピープロテクションシステムの構成が示されている。本例では、パーソナルコンピュータ（以下、PCと略する）の周辺装置として使用されるDVD-RAMドライブに、デジタルコンテンツを暗号化したまま記録するシステムを例示して、その構成を説明する。

【0018】PC11は、IEEE1394シリアルバス200を介して、外部のコンシューマ電子機器、たとえば図示のようなセットトップボックス（STB）12、デジタルビデオカメラまたはDVカムコーダ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14と通信可能に構成されている。

【0019】セットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14は、それぞれIEEE1394シリアルバス200とのインターフェイス部に、デバイス認証およびキー交換などを行う認証処理部（Authenticator）121，131，141を有している。デジタルコンテンツの送受信を行うセットトップボックス（STB）12およびデジタルビデオカセットレコーダ（D-VCR）14については、暗号化・復号化双方の機能を持つ暗号化／復号化部（De-/Cipher）122，142が設けられている。また、デジタルコンテンツの送信のみを行うデジタルビデオカメラ（DVC）13については、暗号化部（Cipher）132だけが設けられている。

【0020】PC11、セットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14間で授受されるデジタルコンテンツは、暗号化された状態でIEEE1394シリアルバス200上を転送される。

【0021】PC11は、図示のように、PCIバス100と、これに接続された複数の機能モジュールとから構成されている。これら機能モジュールの中で、デジタルコンテンツを扱う機能モジュール、つまり、CPUモジュール111、サテライトまたはデジタルTV用のチューナ113、MPEG2デコーダ115、DVD-RAMドライブ116については、PCIバス100とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部（Authenticator）111，1131，1151，1161を有している。これら各認証処理部（Authenticator）111，1131，1151，1161の機能は、基本的に、1394デバイスであるセットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14のそれと同じであり、デジタルコンテンツを暗号化して授受するために必要な認証およびキー交換を行う。

【0022】認証処理部（Authenticato

r)1111, 1131, 1151, 1161内には、それぞれ対応する機能モジュールについての認証情報（認証フォーマット）が保持されている。この認証フォーマットは、コピープロテクト対象のデータを授受する相手先の機能モジュールまたは外部機器に対してその機能モジュールの正当性を証明するために用いられるものであり、一種の電子署名である。認証相手との間で互いのデバイスの認証フォーマットを交換することにより、互いにコピープロテクト対象のデータを扱うことが可能な正当なデバイスであるか否かを確認するための認証処理を機能モジュール毎に行うことが可能となる。

【0023】この認証フォーマットには、対応する機能モジュールの正当性や、扱うことができるデータの種類（コピー不可、一回のみコピー可、コピーフリー）を特定するための情報が含まれている。認証フォーマットは、PC11内の各機能モジュールの回路またはファームウェア、あるいはその機能モジュールに対応するデバイスドライバなどに埋め込まれている。

【0024】また、セットトップボックス（STB）12、ディジタルビデオカメラ（DVC）13、およびディジタルビデオカセットレコーダ（D-VCR）14の認証処理部（Authenticator）121, 131, 141にも、それぞれ対応する機器の認証フォーマットが保持されている。

【0025】CPUモジュール111、チューナ113、MPEG2デコーダ115のインターフェイス部には、さらに、暗号化されたコンテンツ（encrypted contents）の暗号化を解除するための復号化処理を行う復号化部（De-cipher）、または暗号化部（Cipher）が設けられている。暗号化部を持つか復号化部を持つか、あるいはその両方を持つかは各機能モジュールの機能によって決まる。ここでは、チューナ113については暗号化部（Cipher）1132が設けられ、CPUモジュール111およびMPEG2デコーダ115については復号化部（De-cipher）1112, 1152が設けられている場合が例示されている。

【0026】CPUモジュール111は、マイクロプロセッサと、メモリコントローラ、およびPCIバスブリッジなどから構成されており、認証部1111と暗号解除部1112は例えばPCIバスブリッジの一部として組み込むことができる。また、CPUモジュール111内の認証部1111、暗号解除部1112、MPEG2デコーダ部113はソフトウェアで実現しても良い。

【0027】DVD-RAMドライブ116はPC11の補助記憶装置として設けられたものであり、IDEインターフェイスまたはATAPIインターフェイス等を介してPCIバス100に接続される。DVD-RAMドライブ116は認証処理部1161のみを有し、復号化部（De-cipher）、暗号化部（Cipher）については設けられていない。一回のみコピー可の暗号化されたデジタルコンテンツを暗号化した状態のままDVD-RAM116に記録するためである。

【0028】DVD-RAMドライブ116には、再生管理情報付加部1162、および時変情報管理部1163が設けられている。再生管理情報付加部1162は、記録対象の暗号化データに、時刻情報などの特殊再生に必要な再生管理情報を付加する。これにより、暗号化データはそれを構成する所定サイズの暗号化データユニット単位で、暗号化されてない生の再生管理情報が付加された状態でDVD-RAMメディア上のデータ領域に記録される。この場合、各再生管理情報は、対応する暗号化データユニットと他の暗号化データユニットとの間の時間的な順序関係を示す。したがって、再生管理用情報を参照することにより、暗号化データの途中から任意の部分を読み出して再生することができ、早送り再生やマルチシーン再生などの特殊再生時においても、暗号化データ全てを読み出すことなく、その特殊再生に必要な暗号化データ部のみをDVD-RAMメディアから読み出して再生装置側に送信することが可能となる。

【0029】時変情報管理部1163は、各暗号化データユニット毎にその暗号化に使用された時変数の値を特定するための時変要素情報を付加する。このようにして、各暗号化データユニットとそれに対応する時変要素情報とを一緒にパケット化してDVD-RAMメディア上のデータ領域に記録することにより、暗号化データユニットとその復号に必要な時変要素情報を同時に読み出して再生装置側に送信することが可能となる。

【0030】PC11には、さらに、PCIバス100とIEEE1394シリアルバス200間を双方向で接続する1394ブリッジ117が設けられている。1394ブリッジ117には、認証処理部、暗号化部、復号化部はどれも設けられておらず、暗号化されたデジタルコンテンツは暗号化されたままPCIバス100からIEEE1394シリアルバス200へ、またIEEE1394シリアルバス200からPCIバス100へ転送される。このように、1394ブリッジ117は、PC11内の機能モジュールと1394デバイスとの間を透過的に接続する。

【0031】ここで、デジタル衛星放送によるTV番組などのデジタルコンテンツをIEEE1394シリアルバス200を介してSTB12からPC11に取り込み、それをDVD-RAMドライブ116に記録する場合の処理手順について説明する。

【0032】まず、CPU111の制御の下、STB12とDVD-RAMドライブ116との間で機器認証を行い、互いにコピープロテクト機能を有する正当なデバイスであることを確認し合う。この認証処理は、たとえば、ランダムチャレンジ&レスポンス方法や、一方向関数を用いた方法、毎回変わる時変数を使用する方法、あ

るいはこれら方法の組み合わせなどの良く知れた方法を用いて実現される。また、認証処理では、互いの認証フォーマットの交換も行われ、どのようなデータの種類（コピー不可、一回のみコピー化、コピーフリー）を扱えるデバイス同士であるかが確認される。この認証処理には、完全認証と制限付き認証の二つのレベルがあり、認証相手のデバイス同士がどのようなデータの種類を扱えるデバイス同士であるかによって認証レベルが決定される。

【００３３】そして、さらに、この認証処理にて、ＤＶＤ－ＲＡＭドライブ１１６は、ＣＰＵ１１１の制御の下にＳＴＢ１２との間でキー交換を行い、暗号化されたコンテンツの暗号を解除するためのキー（コンテンツキー）を生成するために必要な暗号鍵情報を取得する。

【００３４】ＳＴＢ１２とＤＶＤ－ＲＡＭドライブ１１６との間で互いにコピープロテクト機能を有する正当なデバイスであることが認証されると、ＳＴＢ１２は、デジタルコンテンツを暗号化し、それをＤＶＤ－ＲＡＭドライブ１１６に送る。暗号化されたコンテンツは暗号化されたまま１３９４バス２００およびＰＣＩバス１００を介してＤＶＤ－ＲＡＭドライブ１１６に届き、ＤＶＤ－ＲＡＭドライブ１１６のＤＶＤ－ＲＡＭメディアに暗号化されたまま記録される。この暗号データの記録時には、前述したように記録対象の所定の暗号化データ単位で再生管理情報と時変要素情報が付加される。

【００３５】このように、デジタルコンテンツを扱う複数の機能モジュールそれぞれのインターフェイス部に認証処理部を用意し、機能モジュール間あるいは機能モジュールと外部の１３９４デバイス間でコピープロテクト対象のデジタルコンテンツを受け渡すときに、それらデバイス間で認証処理およびデジタルコンテンツの暗号化・復号化処理を行うことにより、１ＥＥＥ１３９４バス２００およびＰＣＩバス１００のどちらにおいても暗号化解除のためのキー、およびデジタルコンテンツは暗号化されたまま転送されるようになり、デジタルコンテンツの不正コピーを防止することができる。また、各機能モジュールそれぞれの認証処理部は、その機能モジュールに対応するデバイスドライバや、その機能モジュールのハードウェア、あるいはそのハードウェアを制御するためのファームウェアなどによって実現できる。

【００３６】また、ＰＣ１１内の各機能モジュール毎にそれに対応する認証フォーマットを用いて相手側デバイスとの間の認証処理を行っているので、例えば、ＭＰＥＧ２デコーダ１１５については全ての種類のコンテンツ（一回のみコピー可、コピー不可、コピーフリー）を扱えるようにし、ＤＶＤ－ＲＡＭドライブ１１６については一回のみコピー可のコンテンツとコピーフリーのコンテンツのみを扱えるようにするなど、同一ＰＣ内の機能モジュール毎に個々に扱うことが可能なデジタルコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を制限することが可能となる。

【００３７】図２には、図１のシステムにおけるソフトウェアとハードウェアとの関係が示されている。

【００３８】図２において、一点鎖線の上側がソフトウェア、下側がハードウェアである。また、縦方向に階層化されて示されている太枠のブロックがＰＣ１１内の各機能モジュールまたは１３９４デバイスなどのハードウェアデバイスである。

【００３９】Ａｕｔｈｅｎｔｉｃａｔｏｒハンドラは、デジタルコンテンツ再生用ソフトなどのアプリケーションプログラムからの要求に応じて、必要な各ハードウェアデバイスとの間で認証処理やキー交換のための制御を行う。すなわち、このＡｕｔｈｅｎｔｉｃａｔｏｒハンドラの制御の下に、機能モジュール相互間、または機能モジュールと外部機器との間の認証情報の交換が行われ、これによりコピープロテクト対象のデータを扱うことが可能な正当なデバイスであるか否かを確認するための認証処理が行われる。

【００４０】前述したように、１３９４ブリッジ１１７はＰＣ１１内の各機能モジュールと１３９４デバイスとを透過的に接続するので、ＰＣ１１内の各機能モジュールに１３９４デバイスと同様の認証および暗号化・復号化プロトコルを実装することにより、点線で示されているように、アプリケーションプログラムからはＰＣ１１内の各機能モジュールと１３９４デバイスとを区別することなくそれらを等価に扱うことが可能となる。

【００４１】図３には、本実施形態で用いられる認証処理と暗号化処理の手順の一例が示されている。コンテンツを送信する側のデバイスがＳｏｕｒｃｅ Ｄｅｖｉｃｅ（送信ノード）、受信する側のデバイスがＳｉｎｋ Ｄｅｖｉｃｅ（受信ノード）である。

【００４２】Ｓｉｎｋ Ｄｅｖｉｃｅは、まず、認証要求をＳｏｕｒｃｅ Ｄｅｖｉｃｅに渡す。この認証要求には、Ｓｉｎｋ Ｄｅｖｉｃｅの認証フォーマットなどの情報が含まれている。Ｓｏｕｒｃｅ Ｄｅｖｉｃｅは、Ｓｉｎｋ Ｄｅｖｉｃｅが送信対象のコンテンツ（コピー不可、一回のみコピー可、コピーフリー）を扱うことができる正当なコピープロテクト機能を有するデバイスであるか否かを検証する。Ｓｏｕｒｃｅ Ｄｅｖｉｃｅは、Ｓｉｎｋ Ｄｅｖｉｃｅが正当なデバイスであることを確認すると、認証要求に対する応答をＳｉｎｋ Ｄｅｖｉｃｅに返す。この応答には、そのＳｏｕｒｃｅ Ｄｅｖｉｃｅの認証フォーマットなどの情報や、送信対象のデジタルコンテンツがコピー不可、一回のみコピー可、コピーフリーのいずれであるかを示すＣＭＳと称されるコピーコントロール情報（ＥＭＩ）などが含まれている。コピーコントロール情報（ＥＭＩ）の内容は、所定の関数（ｆ［ＥＭＩ］）によって表され、それがＳｉｎｋ Ｄｅｖｉｃｅに送られる。

【００４３】Ｓｉｎｋ Ｄｅｖｉｃｅは、Ｓｏｕｒｃｅ

Deviceの認証フォーマットを用いてそのSource Deviceが正当なコピープロテクト機能を有するデバイスであるか否かを検証する。互いに相手のデバイスが正当なデバイスであることを確認し合うと、今度は、Sink DeviceとSource Deviceとの間で互いに同一の認証キー（Kauth）を共有するためのキー交換処理が実行される。

【0044】次いで、Source Deviceは、乱数を用いてコントロールキー（Kx）を生成し、そのコントロールキーKxを認証キー（Kauth）で暗号化したもの（e［Kx］）をSink Deviceに送信する。Sink Deviceは、暗号化されたコントロールキー（e［Kx］）を認証キー（Kauth）を用いて復号し、コントロールキーKxを生成する。この後、SourceDeviceは、時刻等によって内容が逐次変化する時変数Ncを生成し、それをSink Deviceに送信する。Source Deviceは、

Kx、

f［EMI］、

Nc

の3要素から、コンテンツを暗号化するための暗号化鍵であるコンテンツキー（Kc）を生成する。

【0045】Kc＝j［Kx，f［EMI］，Nc］

なお、詳細は後述するが、実際には、Kxとf［EMI］は合わせて1つの要素として用いられ、

Kc＝j［Kx＋f［EMI］，Nc］

によってコンテンツキー（Kc）が生成される。

【0046】そして、Source Deviceは、コンテンツキー（Kc）を用いてデジタルコンテンツを暗号化し、暗号化データを1394パケットデータの形式でSink Deviceに送信する。Sink Deviceも既にKx、f［EMI］、Ncの3要素を有しているので、コンテンツキー（Kc）を生成することができる。Sink Deviceは、生成したコンテンツキー（Kc）を用いて暗号化データを復号化する

【0047】Source Deviceは、一定時間経過する度にNcの値を更新し、Kc＋1＝j［Kx，f［EMI］，Nc＋1］、具体的には、

Kc＋1＝j［Kx＋f［EMI］，Nc＋1］

を新たなコンテンツキー（Kc）として使用する。そして、Kc＋1で暗号化した暗号化データを送信する。Ncの値が更新されたことは、1394パケットヘッダに含まれる制御情報（Odd／Even bit）によって、Sink Deviceに通知される。Sink Deviceは、Kc＋1を生成し、その生成したKc＋1によって、暗号化データを復号する。

【0048】以下、このようにしてNcの値を更新しながら、デジタルコンテンツの暗号化、暗号化データの送信、復号、が繰り返し行われる。なお、DVD－RAMドライブ116がSink Deviceの場合には、暗号化データの復号は行われず、デジタルコンテンツは暗号化されたままDVD－RAMメディアに記録される。

【0049】次に、図4を参照して、STB12によって受信されたデジタル衛星放送番組などの、一回のみコピー可のデジタルコンテンツを暗号化してDVD－RAMドライブ116に記録する場合の処理手順を説明する。

【0050】なお、DVD－RAMドライブ116は実際にはPCIバス、1394プリッジ117、IEEE1394バスを介してSTB12に接続されるが、1394プリッジ117によってIEEE1394バス200とPCIバス100は互いに透過的に接続されているため、STB12からDVD－RAMドライブ116へのデジタルコンテンツの転送処理、およびその逆の転送処理は、DVD－RAMドライブ116が図示のようにIEEE1394バス200を介してSTB12に接続されて場合と等価に扱うことができる。また、もちろん、DVD－RAMドライブ116自体にIEEE1394バス200とのインターフェイス部を設け、DVD－RAMドライブ116をIEEE1394バス200に直接接続するようにしてもよい。

【0051】（1）STB12とDVD－RAMドライブ116それぞれの認証部（Authnticator）122，1161による認証およびキー交換処理等により、コンテンツキー（Kc）を生成するための3つの要素（Kx、f［EMI］、Nc）がSTB12とDVD－RAMドライブ116との間で共有される。このSTB12とDVD－RAMドライブ116間の認証処理は、CPU111の制御の下で行われる。

【0052】（2）DVD－RAMドライブ116においては、Kx、f［EMI］、Ncは、オペレーティングシステムなどの通常のファイルシステムからは参照できないDVD－RAM上のセクタ間のギャップ領域（セクタヘッダ）に記録される。ここで、実際には、ギャップ領域に記録されるf［EMI］の内容は、「一回のみコピー可」を示す値から「これ以上コピー不可」を示す値に変更される。

【0053】（3）STB12で受信されるデジタル衛星放送番組などのデジタルコンテンツは、MPEG2で圧縮符号化されている。この圧縮符号化されたデジタルコンテンツは、188バイトのMPEG2トランスポートストリームパケット（MPEG2_TSパケット）から構成されている。STB12は、MPEG2_TSパケットをコンテンツキー（Kc）で暗号化し、それを1394パケットにマウントして送信する。

【0054】（4）DVD－RAMドライブ116は、1394パケットを受信すると、そこから暗号化された

MPEG2_TSパケットを取り出す。再生管理情報付加部1162は、暗号化されたMPEG2_TSパケットに対して、特殊再生のためのタイムスタンプ（時刻情報）を再生管理情報として付加する。タイムスタンプは、例えば1セクタ分のデータサイズ単位で付加される。各セクタのタイムスタンプにより、複数のセクタデータそれぞれの間の時間的な順序関係が表される。タイムスタンプとしては、たとえば1394パケットの到着時刻を示す時刻情報を再生管理情報付加部1162によって生成してそれを使用したり、また、STB12から送信される1394パケット内に予めその送信時刻等を示すタイムスタンプがソースパケットヘッダとして付加されている場合には、そのソースパケットヘッダによって与えられるタイムスタンプをそのまま再生管理情報用のタイムスタンプとして使用することもできる。

【0055】（5）時変情報管理部1163は、例えば1セクタ単位で、その暗号化データの暗号化に使用されている時変数を特定するための時変要素情報を付加する。ここで、最初の時変数の値Ncはセクタ間のギャップS領域（セクタヘッダ）などに既に記録されているので、セクタデータに付加する時変要素情報としては、Ncの差分を使用することができる。例えば、時変数の値がNc＋1に変更された場合には、セクタデータに付加すべきNcの差分は、"＋1"である。

【0056】これにより、DVD－RAMメディアに記録される1セクタデータは、図示のように、時変要素情報（Ncの差分）、タイムスタンプ、および暗号化されたMPEG2_TSパケット群から構成されることになる。

【0057】（6）DVD－RAMメディアに暗号化されたまま記録されているデジタルコンテンツを例えばMPEG2デコーダ115やSTB12内蔵のMPEG2デコーダなどで再生する場合には、DVD－RAMドライブ116と再生装置との間の認証およびキー交換処理により、DVD－RAMメディアにデジタルコンテンツを記録するときに使用したコンテンツキーKcと同一のコンテンツキーKcの生成は、DVD－RAMメディアのギャップ領域に記録されているKx、f［EMI］、Ncを基に行われる。しかし、DVD－RAMメディアのf［EMI］の内容は前述したように「一回のみコピー可」を示す値から"これ以上コピー不可"を示す値に既に変更されているので、同一のコンテンツキーKcを再生装置側で生成できるようにするためには、f［EMI］の変更分が相殺されるような新たなコントロールキーKx'を再生装置側で生成できるようにすることが必要となる。そのために、DVD－RAMドライブ116は、乱数によってコントロールキーKx'を生成するのではなく、DVD－RAMメディアのギャップ領域に記録されている以前のKxに基づいて、新たなコントロールキーKx'を生成する。具体的には、

Kx＋f［一回のみコピー可］　＝　Kx'＋f［これ以上コピー不可］

となるようなKx'を生成する。

【0058】これにより、Kc＝｝［Kx＋f［EMI］，Nc］の関数を利用してコンテンツキーを生成すれば、DVD－RAMメディアにデジタルコンテンツを記録するときに使用したコンテンツキーKcと同一のコンテンツキーKcを生成することが可能となる。

【0059】なお、再生管理情報付加部1162および時変情報管理部1163は、DVD－RAMドライブ116内のハードウェア、DVD－RAMドライブ116を制御するためのデバイスドライバ、あるいはDVD－RAMドライブ116内のマイコン制御用のファームウェアなどによって実現することができる。

【0060】次に、図5を参照して、DVD－RAMメディア上にデジタルコンテンツを記録する場合の具体的なデータフォーマット（記録形式）について説明する。

【0061】前述したように、DVD－RAMメディア上のセクタ間のギャップ領域には、Kx、f［EMI］、Ncが記録される。この場合、f［EMI］の内容は"1回のみコピー可"から"これ以上コピー不可"の状態に変更された状態で記録される。

【0062】DVD－RAMメディアの1セクタのデータサイズは2Kバイトである。図5（A）に示されているように、2Kバイトのセクタデータの先頭には時変要素情報（Ncの差分）が位置され、それに後続してタイムスタンプ（再生管理情報）が位置される。タイムスタンプの後には、188バイトの暗号化されたMPEG2_TSパケット群が後続する。このようにDVD－RAMメディアのアクセス単位となるセクタ毎にクイムスタンプを付加して記録することにより、そのクイムスタンプを参照して、再生対象のデータのみを効率良く読み出すことが可能となる。例えば、早送り再生の場合には、一定時間間隔おきのタイムスタンプを有するセクタを順次選択し、選択された各セクタ内から暗号化されたMPEG2_TSパケットが読み出される。

【0063】また、時変要素情報（Ncの差分）が各セクタデータに付加されているので、暗号化されたMPEG2_TSパケットを読み出しながら、その暗号化解除のために必要なNcの内容を再生装置側に通知することができる。

【0064】図5（B）は、STB12から受信した1394パケット内に付加されているソースパケットヘッダによって与えられるタイムスタンプをそのまま再生管理情報用のタイムスタンプとして使用した場合のセクタデータのフォーマットである。この場合、2Kバイトのセクタデータの先頭には時変要素情報（Ncの差分）が位置され、その後に、4バイトのソースパケットヘッダ（SPH）と188バイトの暗号化された前PEG2_

TSパケットとの組が、後続される。つまり、ソースパケットヘッダを含む1394パケットにおいては、1394パケットのペイロード部は、4バイトのソースパケットヘッダ（SPH）と188バイトの暗号化されたMPEG2_TSパケットとの合計192バイトのデータから構成されており、その192バイトの1394パケットペイロード群がそのまま時変要素情報（Ncの差分）に該当される。

【0065】ここで、図6を参照して、STB12から送信される1394パケットの構造について具体的に説明する。

【0066】STB12は、送信対象のMPEG2_TSパケットをアイソクロナス転送用の1394パケットにマウントする。MPEG2_TSパケットは前述したように188バイトの固定長パケットであり、ここには動画データのビットストリームと音声データのビットストリームが多重化されている。STB12は、このMPEG2_TSパケットに対して、IEC61883で規定された4バイトのソースパケットヘッダ（SPH）を付加する、ソースパケットヘッダ（SPH）は、1394パケット間に伝送遅延差が生じることによる問題を解決するために付加されるタイムスタンプであり、伝送遅延差を補償するための所定の時刻情報から構成される、通常は、送信ノードによるパケット送信時刻などがソースパケットヘッダとして付加される。このソースパケットヘッダを付加して送信することにより、パケットの到着順序がずれても受信側で正しい順序に並べ替えることができる。また、ソースパケットヘッダで与えられるタイムスタンプにより受信側でのパケット復元時刻を指定することができる。つまり、パケット送信時刻等からなるタイムスタンプはパケット復元時刻を指定する時刻情報として使用される。この場合、受信側では、受信したパケットをバッファリングし、ソースパケットヘッダで与えられるタイムスタンプに合わせて復元することにより、パケット毎に異なる伝送遅延が生じた場合でも、正しいタイミングでビデオやオーディオなどのデジタルコンテンツを復号・再生することができる。

【0067】そして、STB12は、ソースパケットヘッダ（SPH）とMPEG2_TSパケットから構成される192バイトのデータの先頭にアイソクロナス転送用の1394パケットヘッダを付加して、1394パケットを生成する。この1394パケットヘッダには、Ncの変化の有無を示すOdd／Even bitも含まれている。生成された1394パケットは、125μsのアイソクロナスサイクル内に1つの割合で転送される。

【0068】このように、暗号化されたデジタルコンテンツは、パケット送信時刻などを示すタイムスタンプがそれぞれに付加された複数の1394パケットに分割されてSTB12から送信されるので、図5（B）のように、そのタイムスタンプを再生管理情報用のタイムスタンプとしてそのまま使用することにより、DVD－RAMドライブ116内で1394パケットの到着時刻を基に専用のタイプスタンプを生成するといった処理が不要となる。

【0069】図7には、STB12で暗号化のために使用されるNcの変化とセクタデータの先頭に記録される時変要素情報（Ncの差分）の値との関係が示されている。

【0070】前述したように、1394パケットヘッダのOdd／Even bitの値は、Ncの値が更新されるする度に変化する。具体的には、Odd／Even bitの値は、実際に使用したNcの最下位ビットの値に相当する。Ncの値が増えるとOdd／Even bitの値も変化するので、受信ノードは、Ncの値が増加したことを知ることができる。

【0071】したがって、最初に送信ノードから通知されたNcの値が変化するまでは、Odd／Even bitの値は変化せず、セクタデータの先頭に記録される時変要素情報（Ncの差分）は“0”となる。Ncの値がNc＋1に増えると、Odd／Even bitの値が変化し、セクタデータの先頭に記録される時変要素情報（Ncの差分）は“＋1”となる、さらに、Ncの値がNc＋2に増えると、Odd／Even bitの値が再び変化し、セクタデータの先頭に記録される時変要素情報（Ncの差分）は“＋2”となる。

【0072】次に、図8を参照して、MPEG2_TSパケットをDVD－RAMドライブ116に記録する場合の一連の処理手順を説明する。

【0073】ここでは、前述と同様にSTB12がデジタル衛星放送受信機として動作する場合を想定する。

【0074】STB12は、アンテナを介してMPEG2_TSパケットを受信すると（ステップS11）、そのMPEG2_TSパケットの先頭にIEC61883で規定されている前述のソースパケットヘッダ（SPH）を付加する（ステップS12）。この後、STB12は、さらに先頭に、Odd／Even bitを含む1394パケットヘッダを付加して、アイソクロナス転送用の1394パケットを作成する（ステップS13）。この1394パケットの作成時に、MPEG2_TSパケットの暗号化が行われる、この暗号化には、DVD－RAMドライブ116との間の認証及びキー交換処理で生成したコンテンツキーが用いられる。1394パケットヘッダおよびソースパケットヘッダ（SPH）は暗号化されない。そして、STB12は、1394パケットをDVD－RAMドライブ116宛に送信する（ステップS14）。

【0075】DVD－RAMドライブ116は、1394パケットを受信する（ステップS15）。そして、DVD－RAMドライブ116は、受信した1394パケットの1394パケットヘッダ内に含まれているOdd

／Ｅｖｅｎ　ｂｉｔを参照してＮｃの変化の有無を確認し、Ｎｃの差分を生成する（ステップＳ１６）。この後、ＤＶＤ－ＲＡＭドライブ１１６は、受信した１３９４パケットから１３９４パケットヘッダを取り除き、Ｎｃの差分の後に、１３９４パケットペイロード部を付加する（ステップＳ１７）。この場合、Ｎｃの差分が同じであるパケットペイロード同士が集められ、２Ｋバイト以下のデータサイズを有するセクタ書き込み用パケットが生成される。なお、ここでは、ソースパケットヘッダ（ＳＰＨ）を再生管理情報用のタイムスタンプとしてそのまま流用したので、セクタ書き込み用パケットにＳＰＨが複数含まれているが、基本的には、１つのセクタ書き込み用パケットに１つの目印となるＳＰＨが付加されていればよい。よって、連続のＳＰＨのうちの１つを選択してそれをセクタ書き込み用パケットに付加することも可能である。この後、ＤＶＤ－ＲＡＭドライブ１１６は、作成したセクタ書き込み用パケットをＤＶＤ－ＲＡＭメディア上の書き込み対象のセクタ位置に書き込む（ステップＳ１８）。

【００７６】このようにして、所定のデータサイズ単位でＮｃの差分とタイムスタンプとが付加された状態で暗号化データが記録されていく。

【００７７】次に、図９を参照して、ＤＶＤ－ＲＡＭドライブ１１６に記録されたＭＰＥＧ２＿ＴＳパケットを再生する場合の一連の処理手順を説明する。

【００７８】ここでは、ＤＶＤ－ＲＡＭドライブ１１６に記録されたＭＰＥＧ２＿ＴＳパケットをＳＴＢ１２で再生する場合を想定する。

【００７９】まず、ＤＶＤ－ＲＡＭドライブ１１６は、ＣＰＵ１１１によって実行される再生制御ソフトウェアやＤＶＤ－ＲＡＭドライブ１１６用のデバイスドライバなどによって指定された再生対象のデータ部を記録しているセクタを、ＳＰＨの値を目安にして検索し、該当するセクタデータをＤＶＤ－ＲＡＭメディアからリードする（ステップＳ２１）。そして、読み出したセクタデータに対応するＮｃの差分を確認しながら、１３９４パケットを生成する（ステップＳ２３，２４）　Ｎｃの差分の値はセクタデータの先頭に付加されているので、一回のセクタデータ読み出しで、該当するＮｃの差分値を確認することができる。Ｎｃの差分値が同一であるものについては、１３９４パケットヘッダのＯｄｄ／Ｅｖｅｎ　ｂｉｔの値は同じになる。このようにして生成された１３９４パケットは、ＩＥＥＥ１３９４バス経由でＳＴＢ１２に送信される（ステップＳ２５）。ＳＰＨは新たに生成し直すようにしてもよい。

【００８０】また、このような１３９４パケットの生成処理は、ＣＰＵ１１１によって実行されるソフトウェアによって行うようにしてもよい。

【００８１】ＳＴＢ１２は、１３９４パケットを受信すると（ステップＳ２６）、その１３９４パケットから暗号化されたＭＰＥＧ２＿ＴＳパケットを取り出し、その暗号化を解除するための復号処理を行った後、そのＭＰＥＧ２＿ＴＳパケットをデコードして再生する（ステップＳ２７）。

【００８２】

【発明の効果】以上説明したように、本発明によれば、暗号化データに再生管理用情報を付加してデジタル記録しているため、その再生管理用情報を参照することにより、暗号化データの途中から任意の部分を読み出して再生することができる。したがって、早送り再生、早送り逆再生、マルチシーン再生などの特殊再生時においても、暗号化データ全てを読み出すことなく、その特殊再生に必要な暗号化データ部のみを記録媒体から読み出して再生装置側に送信することが可能となる。また、暗号化データとそれに対応する時変要素情報とをパケット化して記録することにより、時変要素値を暗号化鍵として使用するコピープロテクションシステムにおいても、暗号化データユニットとその復号に必要な時変要素情報とを同時に読み出して再生装置側に送信することが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るパーソナルコンピュータのシステム構成を示すブロック図。

【図２】図１のシステムにおけるソフトウェアとハードウェアとの関係を示す図。

【図３】同実施形態で用いられる認証及び暗号化処理の手順を示す図。

【図４】同実施形態で用いられるＳＴＢとＤＶＤ－ＲＡＭドライブとの間で実行される処理を説明するための図。

【図５】同実施形態で用いられるデジタルコンテンツの記録形式の一例を示す図。

【図６】同実施形態で用いられる１３９４パケットの構造を示す図。

【図７】同実施形態におけるＮｃの変化とセクタデータの先頭に記録される時変要素情報（Ｎｃの差分）の値との関係を示す図。

【図８】同実施形態においてＭＰＥＧ２＿ＴＳパケットをＤＶＤ－ＲＡＭドライブに記録する場合の一連の処理手順を示す図。

【図９】同実施形態においてＭＰＥＧ２＿ＴＳパケットを再生する場合の一連の処理手順を示す図。

【符号の説明】

１１…パーソナルコンピュータ（ＰＣ）

１２…セットトップボックス（ＳＴＢ）

１３…デジタルビデオカメラまたはＤＶカムコーダ（ＤＶＣ）

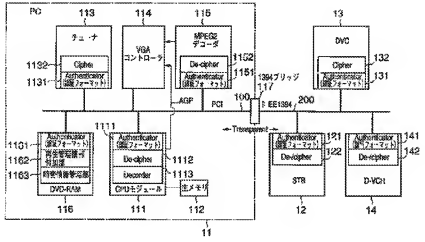
１４…デジタルビデオカセットレコーダ（Ｄ－ＶＣＲ）

１１１…ＣＰＵモジュール

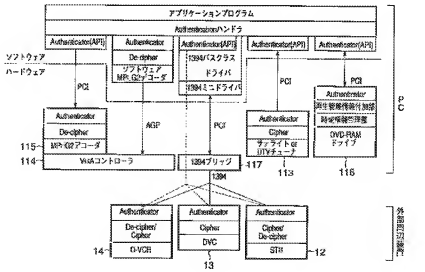
１１２…主メモリ

113…サイライトまたはデジタルTVチューナ
114…VGAコントローラ
115…MPEG2デコーダ
116…DVD-RAMドライブ
117…1394ブリッジ
121…認証部(Authenticator)
122…暗号化・復号化部(De-/Cipher)
131…認証部(Authenticator)
132…暗号化部(Cipher)
141…認証部(Authenticator)
142…暗号化・復号化部(De-/Cipher)
111…認証部(Authenticator)
112…復号化部(De-cipher)
1131…認証部(Authenticator)
1132…暗号化部(Cipher)
1151…認証部(Authenticator)
1152…復号化部(De-cipher)
1161…認証部(Authenticator)
1162…再生管理情報付加部
1163…時変情報管理部

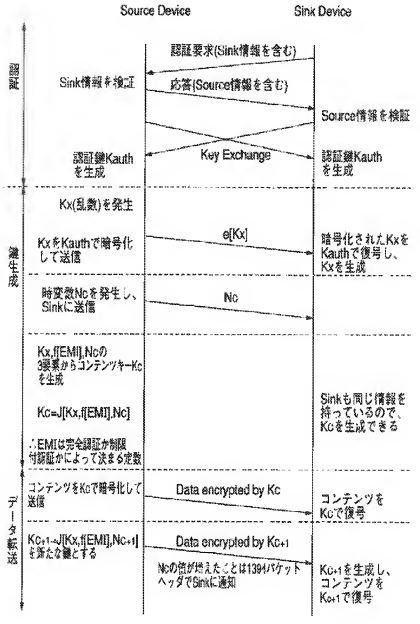
【図1】



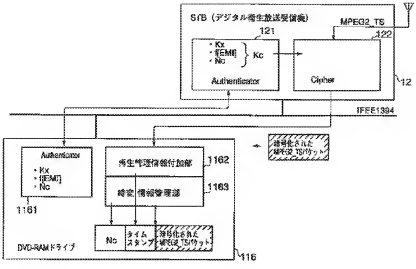
【図2】



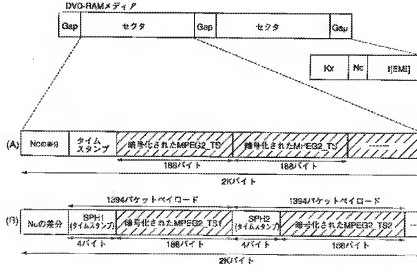
【図3】


Source Device
Sink Device
認証
鍵生成
データ転送
認証要求(Sink情報を含む)
Sink情報を検証
応答(Source情報を含む)
Source情報を検証
認証鍵Kauth
を生成
Key Exchange
認証鍵Kauth
を生成
Kx(乱数)を発生
Kxを Kauthで暗号化
して送信
e[Kx]
暗号化されたKxを
Kauthで復号し、
Kxを生成
時変数Ncを発生し、
Sinkに送信
Nc
Kx,f[EMI],Ncの
3要素からコンテンツキーKc
を生成
Kc=J[Kx,f[EMI],Nc]
Sinkも同じ情報を
持っているので、
Kcを生成できる
∴EMIは完全認証か制限
付認証かによって決まる定数
コンテンツをKcで暗号化して
送信
Data encrypted by Kc
コンテンツを
Kcで復号
Kc+1=J[Kx,f[EMI],Nc+1]
を新たな鍵とする
Data encrypted by Kc+1
Ncの値が増えたことは1394パケット
ヘッダでSinkに通知
Kc+1を生成し、
コンテンツを
Kc+1で復号

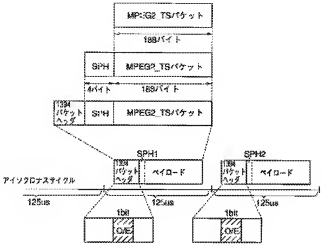
【図4】


STB（デジタル衛生放送受信機）
MPEG2_TS
121
122
・Kx
・f(EMI)
・Nc
Kc
Authentication
Cipher
12
IEEE1394
Authenticator
・Kx
・f(EMI)
・Nc
1161
再生制御情報付加部
1162
暗号 情報管理部
1163
暗号化された MPEG2 TSパケット
Nc
タイム スタンプ
暗号化された MPEG2 TSパケット
DVD-RAMドライブ
116

【図5】


DVD-RAMメディア
Gap
セクタ
Gap
セクタ
Gap
Kx
Nc
f(EMI)
(A)
Ncの差分
タイム スタンプ
暗号化されたMPEG2_TS
暗号化されたMPEG2_TS
188バイト
188バイト
2Kバイト
1394パケットペイロード
1394パケットペイロード
(B)
Ncの差分
SPH1 (タイムスタンプ)
暗号化されたMPEG2_TS1
SPH2 (タイムスタンプ)
暗号化されたMPEG2_TS2
4バイト
188バイト
4バイト
188バイト
2Kバイト

【図6】



【図7】

SourceのNc	Odd/Even Bit	HVD-RAM上のSectorの先頭に記録する時変情報
		Ncの差分
Nc	O/E=0	0
Nc	O/E=0	0
Nc+1	O/E=1	+1
Nc+2	O/E=0	+2
Nc+2	O/E=0	+2

【図8】

MPEG2_TSを記録するときのフロー
STB側の処理
S11
MPEG2_TSパケット受信
S12
SPHを付加(IEC61883)
S13
1394パケットヘッダ付加
S14
STBから送信
DVD-RAM側の処理
S15
DVD-RAM受信
S16
1394パケットヘッダを参照しNcの変化を確認
S17
1394パケットヘッダを取り除きNcの差分とペイロード部をパケット化
S18
記録
パケット変化フロー
MPEG2_TSパケット
SPH
MPEG2_TSパケット
この時に暗号化
1394パケットヘッダ
SPH
暗号化されたMPEG2_TSパケット
1394パケットヘッダ
SPH
暗号化されたMPEG2_TSパケット
ここを参照してNcの差分を生成する
●Ncの値が同じであるパケットを集める
Ncの差分
SPH
暗号化されたMPEG2_TSパケット
SPH
暗号化されたMPEG2_TSパケット
2Kbyte以下(DVD-RAMのセクタサイズ)

【図9】

MPEG2_TSを再生するときのフロー
パケット変化フロー
SPHの値で目安をつけて、目的のパケットをディスクから読み出す
S21
S22
S23
S24
S25
S26
S27
DVD-RAM機の処理
STB機の処理
指定されたSPHのあるパケットを探索
ディスクからのパケット読み込み
Nc0の差分を蓄積
ディスクのパケットを分離し1394パケットを生成
DVD-RAM送信
STB受信
復号化・再生
Nc0の差分
SPH
暗号化されたMPEG2 TSパケット
Nc0の差分をパケット内に記録しているため、このプロセスを6つの1個の値の読み込みで行うことができる。
1394パケットヘッダ
Nc0の差分が異なるものについては1394パケットヘッダのOdd/Even bitの値は異なる。
MPEG2_TS
Odd/Even bitが変化する